

cific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(iv) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(v) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iii) or any of the offenses listed in—

(I) sections 1028 through 1030 of title 18 (relating to fraud and identity theft);

(II) chapter 37 of such title (relating to espionage and censorship); and

(III) chapter 90 of such title (relating to protection of trade secrets).

(B) Prohibited activities

Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) Privacy and civil liberties

Cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain—

(I) personal information of a specific individual; or

(II) information that identifies a specific individual; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing—

(I) personal information of a specific individual; or

(II) information that identifies a specific individual.

(D) Federal regulatory authority

(i) In general

Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this subchapter shall not be used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any non-Federal entity or any activities taken by a non-Federal entity pursuant to mandatory standards, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.

(ii) Exceptions

(I) Regulatory authority specifically relating to prevention or mitigation of cybersecurity threats

Cyber threat indicators and defensive measures provided to the Federal Gov-

ernment under this subchapter may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.

(II) Procedures developed and implemented under this subchapter

Clause (i) shall not apply to procedures developed and implemented under this subchapter.

(Pub. L. 114–113, div. N, title I, § 105, Dec. 18, 2015, 129 Stat. 2943.)

§ 1505. Protection from liability

(a) Monitoring of information systems

No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 1503(a) of this title that is conducted in accordance with this subchapter.

(b) Sharing or receipt of cyber threat indicators

No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 1503(c) of this title if—

(1) such sharing or receipt is conducted in accordance with this subchapter; and

(2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 1504(c)(1)(B) of this title and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 1504(a)(1) of this title and guidelines are submitted to Congress under section 1504(b)(1) of this title; or

(B) the date that is 60 days after December 18, 2015.

(c) Construction

Nothing in this subchapter shall be construed—

(1) to create—

(A) a duty to share a cyber threat indicator or defensive measure; or

(B) a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure; or

(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(Pub. L. 114–113, div. N, title I, § 106, Dec. 18, 2015, 129 Stat. 2950.)

§ 1506. Oversight of government activities

(a) Report on implementation

(1) In general

Not later than 1 year after December 18, 2015, the heads of the appropriate Federal enti-